

Figure 1a

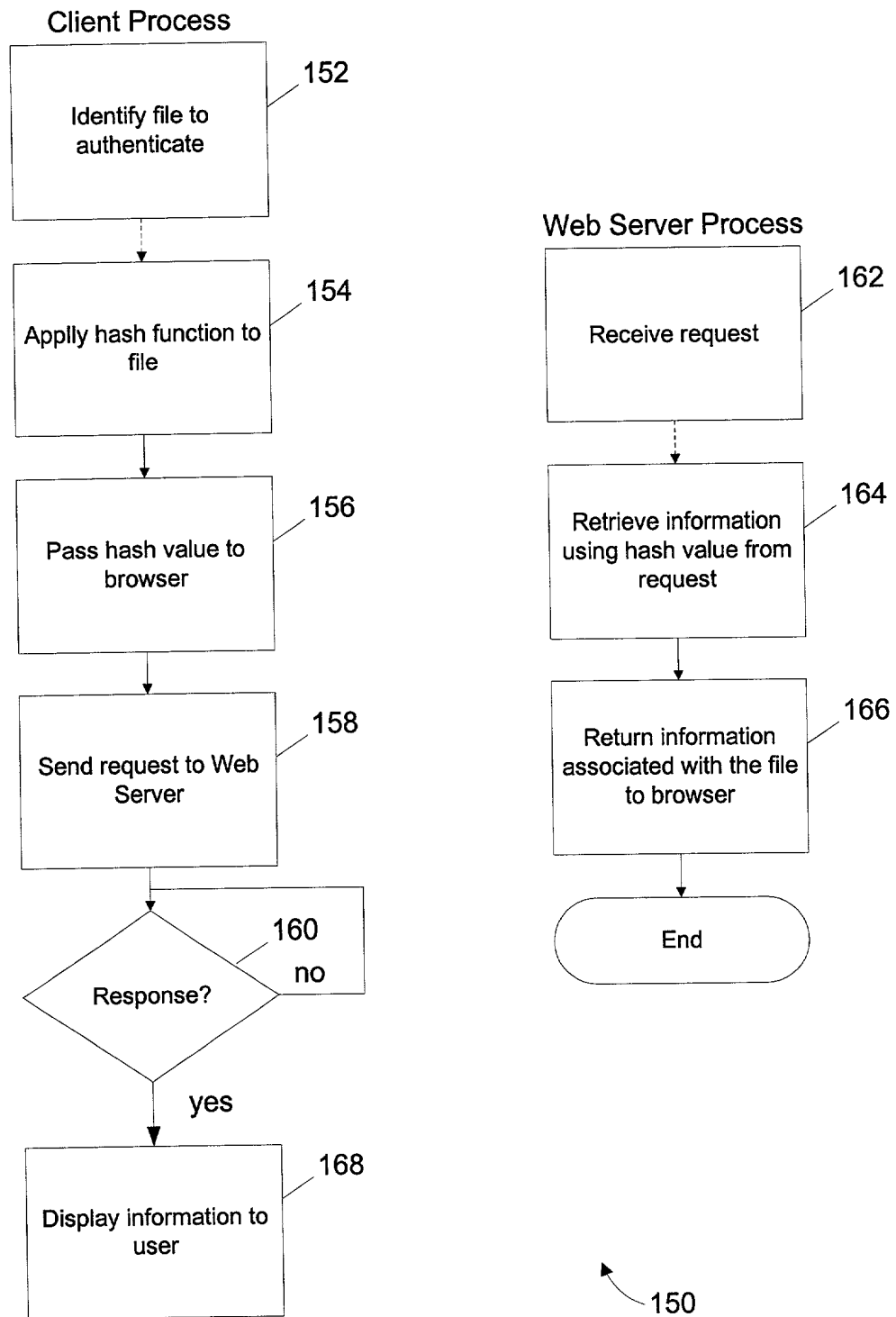


Figure 1b

**Example A: An authentic file.**

**Internet File Safety Information Center**

**File Name: ZixMailSetup.exe      Author: ZixIt Corporation**

**File Hash: 0123456789ABCDEF0123456789ABCDEF**

**The authenticity of this file has been verified by comparing with an authentic file directly obtained from the author.**

**Test Result: No virus discovered. No malicious behavior detected.**

**20,237,393 users have looked up the information about this file. None have reported any malicious behavior.**

**Example B: An unknown file.**

**Internet File Safety Information Center**

**File Hash: ABCDEF0123456789ABCDEF0123456789**

**No other information available.**

**10 users have looked up the information about this file. None have reported any malicious behavior.**

**We cannot determine whether the file is authentic. Please be cautious when using this file.**

**Example C: A file known to be malicious**

**Internet File Safety Information Center**

**File Hash: DEF01234567890123456789ABCABCDEF**

**WARNING!!! This file is a dangerous Trojan horse. It will wipe out you hard drive. DO NOT RUN IT!**

**23,789 users have looked up the information about this file. 5 users have reported extremely dangerous malicious behavior. Our lab test has confirmed such a behavior. For more information click:**

**<http://www.filesafetycenter.com/malicious/PKZ300TROJ.html>**

**Figure 2**